Final

MODELING THE OPTICAL ENCRYPTION PROCESS

By Deborah Jackson
Jet Propulsion Laboratory
California Institute of Technology

The internet is a rapidly growing communications forum which presents problems to some to its potential users, because of its inability to secure, unconditionally, information transferred through its channels. This has particular importance for large, geographically disbursed institutions that would like to take advantage of publicly available multi-media channels to conduct low cost, day to day business transactions. Throughput data rates for completing DES based encryption/decryption processing are currently possible at 1 Gbps using application specific integrated circuits. This is close to the limit of what can be achieved electronically. Thus, with the anticipated introduction of wideband, all-optical networks and their attendant data rates (from 10 Gbps up to 1 Tbps), user requirements to encrypt and decrypt information will tend to limit the useful bandwidth that can be exploited in all optical networks. My research has explored the use of an optical encryption scheme to remove the bottleneck, by allowing faster data throughput.

In an optical encryption/decryption scheme, plaintext (in serial digital format) is converted to a two dimensional image format which is readout as an optical image. It is as an image that the information is encrypted via large scale optical parallel processing. The enciphered output (ciphertext) is then converted back to a serial data stream. This approach has the potential for achieving high data rates as well as allowing the use of very large encryption keys. But in encryption applications, it is important to recover all of the original plaintext, with no errors, after going through a full encrypt/decrypt cycle. The feasibility of this encryption approach thus depends on understanding how much bandwidth expansion is required of the ciphertext to achieve an acceptable bit error rate (BER). The latter depends very much on the intrinsic characteristics of the optical devices used to encrypt the data.

A block diagram of the physical setup is shown in Figure 1. The SCRAM is a black box that converts a serial data stream into a 2-dimensional format which is eventually read-out as an image. After undergoing a phase scrambling optical transform, this output (scrambled) image is captured and digitized. It is the scrambled bits that are then transmitted to the internet.

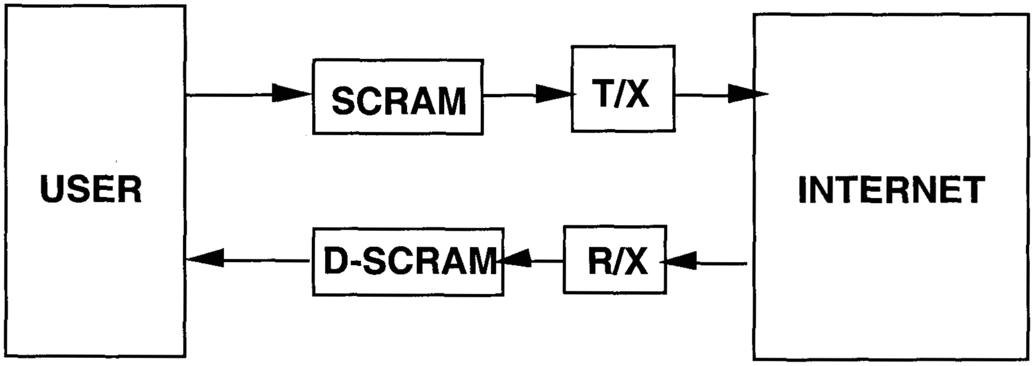

Figure 1. Schematic depicting insertion of optical encryption scrambler (SCRAM) and optical decryption de-scrambler (DSCRAM) between the Internet and the user.

Figure 2 gives a more detailed flow diagram of the data scrambling sequence. The user is seeking to transmit a string of digital packet, but needs to encrypt them before transmitting on the internet. The packets, which are made up of the digital data stream and the packet header, are thus loaded into the Spatial Light Modulator (SLM) in the SCRAM, by filling it up line by line with one byte per pixel.

This 2-dimensional spatial display is then optically read out using an optical source. The free space optical read-out is then scrambled by random phase shifts at a second spatial light modulator. That is, the spatial light modulator is used to individually offset the phase at each pixel by a random amount. The hologram of the distorted image is captured on a CCD, the contents of which are read out line by line. At this point, an external header is added to the encrypted data. Finally, before transmission, the error coding is added.

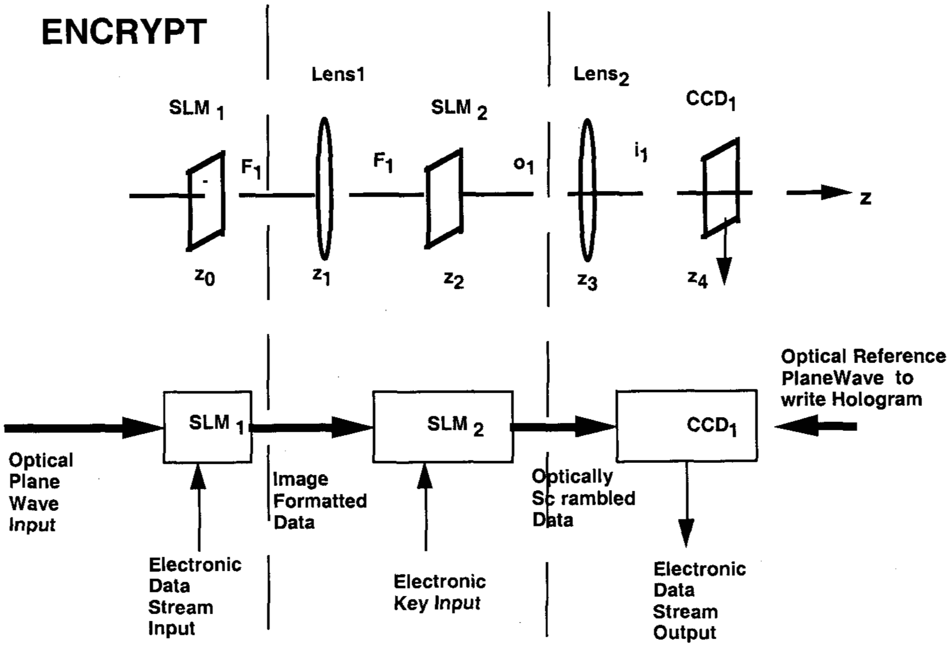

Figure 2. Data encryption flow diagram preparing for internet transmission.

To recover the signal, the reverse process is employed at a DSCRAM unit. Upon receipt from the internet, the DSCRAM error checks the packet, strips the external header, then loads the serial data stream in tile proper sequence into a recovery SLM.

Our analysis has shown that acceptable BER's can be achieve if stray light can be reduced to a level that falls below the shot noise fluctuations of the light source. A carefully designed system that meets these two design requirements has tremendous potential for providing high speed encryption for internet users.

The research described in this publication was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the NSA.